ASCP NPQR
NATIONAL PATHOLOGY QUALITY REGISTRY

National Pathology Quality Registry:

Ensuring Privacy and Security for You and Your Patients

www.ascp.org/NPQR

“ The NPQR is a flexible, dynamic tool designed by those of us in the laboratory, for us. With the NPQR, ASCP and our members are able to improve the quality of what we do, demonstrate the value we add, and elevate the care we provide to our patients.”

Ali Brown, MD, FASCP
Chief Officer, Medical Quality, ASCP

ASCP NPQR
NATIONAL PATHOLOGY QUALITY REGISTRY

Table of Contents

Introduction

The storage of electronic data has been a game changer in modern healthcare. It has given rise to the field of informatics, in which large quantities of data help providers manage the health and wellness of populations as well as improve the quality and safety of patient care. As electronic health records (EHRs) are collecting vast amounts of data, protecting patient privacy and healthcare data security and strict adherence to Health Insurance Portability and Accountability Act (HIPAA) regulations are paramount. The National Pathology Quality Registry (NPQR)—a national quality and benchmarking program established in 2017 by the American Society for Clinical Pathology ASCP)—addresses these issues, which are worth discussing in depth:

- **Privacy**
- **Security**
- **Compliance**

The NPQR captures data that measure adherence to clinical practice guideline recommendations, quality and performance standards, and appropriate utilization of laboratory testing. The NPQR provides support for pathologists and lab professionals to drive improvement through the use of real-time data analytics from their own laboratories, integrated with national and peer group comparisons.

In addition, the NPQR has been granted QCDR (Qualified Clinical Data Registry) status by the Centers for Medicare and Medicaid Services, meaning pathologists and laboratories can use the NPQR to harness their data to both improve patient care and fulfill MIPS (Merit-Based Incentive Payment System) requirements.

Ensuring patient privacy and data security is critical in this digital age where cyber-criminals are developing increasingly sophisticated tools and methods to attack healthcare organizations. Through protecting patient privacy, ensuring healthcare data security, and adherence to HIPAA regulations, the NPQR offers an opportunity to safely and securely drive improvement.

Protecting Patient Privacy

Securing Your Data

As you prepare to share data with a registry to benchmark your institution's performance with peer institutions, it's important to understand how your data are being used and shared since EHRs can make data vulnerable to internal or external agents.

How the ASCP NPQR Uses Your Data

ASCP, as a company, will not sell your patient data to third parties. The NPQR platform utilizes technology developed by leaders in clinical data exchange and analytics. Data that we collect can include a patient's name, date of birth, zip code, laboratory order and result dates, medical record number, payer, and other case-level treatment and outcome data. Data collected do not include phone number, street address, fax, email address, medical claim number, or other information regarding payment.

Ensuring Data Security

Healthcare data are valuable to cyber-criminals. You can reduce your potential exposure when working with a registry by ensuring the registry restricts access and uses encryption and regular security audits.

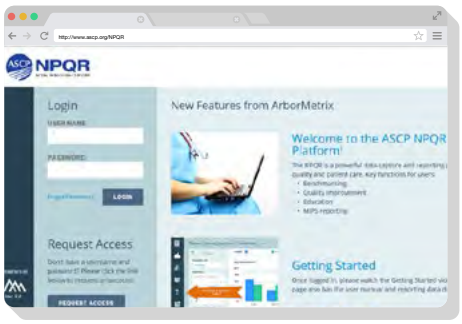
Restricted Access

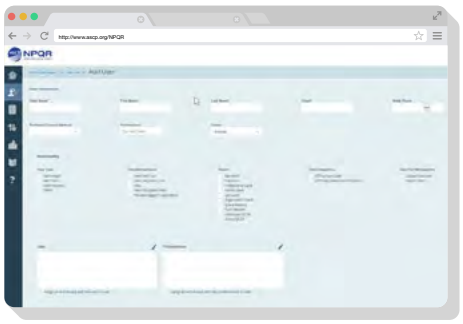
Best practices for securing access control include the following:

1. Dividing data into categories, based on whether they should be publicly available or are sensitive in nature.
2. Making sure sensitive data are protected and can only be accessed by authorized employees who have a legitimate purpose for use.
3. Restricting data access strictly to what's required for each job role.

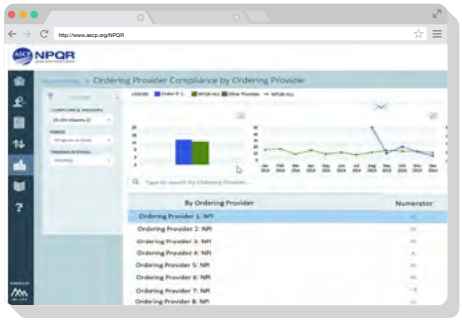
The NPQR aligns with these practices in the following ways:

1. User access is managed by role-based permissions.





2. Access rights are restricted to the least privileges necessary to perform the job, which are determined by the participating site.
3. Users from participating laboratories who have a user account for the registry can only view the patient-level data from their own laboratory.
4. For benchmarking purposes, laboratories only have access to de-identified aggregate data without protected health information (PHI) from other sites.



Use of Encryption

Encryption of data is important when sensitive data must be sent across open networks. Data encryption prevents data visibility in the event of unauthorized access or theft. It is commonly used to protect data in motion and is increasingly promoted for protecting data at rest.

Best practices for encrypting data include the following:

1. Identifying sensitive data, and ensuring encryption at all times—in transit and at rest.
2. Only including strong encryption methods in encryption of data at rest.
3. Using best practices to properly authenticate a person's identification and authorize features of the software.
4. Creating audit logs that can be scanned for suspicious behavior.

The NPQR's solutions follow the latest best practices, including encryption of data at rest, on both database and file systems, and while in transit.

Use of Audits

Auditing who accesses data and what they do with it is an important step in protecting patients.

Important details to keep in mind relating to the use of audits include the following:

1. HIPAA requires having an audit trail, although the degree of detail kept in audit logs can vary by what the organization considers useful.
2. Patients have the right to request additional protection for their information, so the system used for auditing access must be flexible enough to take that into account.

The NPQR's vendors submit to regular security audits by third parties.

Complying with HIPAA Regulations

HIPAA Identifiers

1. Names
2. All geographical subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the HIPAA covered entity to code the data)

There are additional standards and criteria to protect individuals' privacy from re-identification. Any code used to replace the identifiers in datasets cannot be derived from any information related to the individual and the master codes, nor can the method to derive the codes be disclosed. For example, a subject's initials cannot be used to code their data because the initials are derived from their name. Additionally, the covered entity must not have actual knowledge that the individual could be re-identified from the remaining identifiers in the PHI used. In other words, the information would still be considered identifiable if there was a way to identify the individual, even though all of the 18 identifiers were removed.

HIPAA

Healthcare providers who electronically transmit any health information in connection with transactions for which the U.S. Department of Health and Human Services has adopted standards are required to adhere to HIPAA Rules. **The HIPAA Security Rule** requires healthcare providers to assess data security controls by conducting a risk assessment, and to implement a risk management program to address any vulnerabilities.

The HIPAA Security Rule outlines policies to protect all individually identifiable health information that is transmitted. These are the 18 HIPAA Identifiers that are considered personally identifiable information. This information can be used to identify, contact, or locate a single person, or can be used with other sources to identify a single individual. When personally identifiable information is used in conjunction with one's physical or mental health or condition, health care, or one's payment for that health care, it becomes protected health information (PHI). The HIPAA Security Rule describes what covered entities must do to secure electronic PHI. All HIPAA covered entities that collect, maintain, use, and transmit electronic PHI must adopt certain technical and non-technical safeguards to protect it.

The NPQR complies with HIPAA regulations by implementing safeguards to protect sensitive personal and health information.

Conclusion

Patient confidentiality is one of the most important pillars of medicine. Protecting patient data is essential in retaining trust between your healthcare system and your patients. Actionable data analytics are critical to health care, and registries are a vital resource for quality improvement data. Registries enable hospitals, health systems, and physicians to assess the effectiveness of their practices and advance efforts to deliver data-driven, evidence-based care.

The NPQR aggregates data from both clinical and anatomic pathology laboratory information systems to provide timely reports as well as provide interactive dashboards that allow laboratories to analyze their performance while ensuring privacy and security. Participants can then share reports with frontline staff, departments, practice managers, and hospital administrators, allowing pathologists and laboratory professionals to take a lead role in quality management at their institutions.

About the NPQR

The NPQR is a national quality and benchmarking program led by ASCP, the world's largest professional membership association for pathologists and laboratory professionals. The registry captures data that measure adherence to clinical practice guideline recommendations, quality and performance standards, and appropriate utilization of laboratory testing.

Learn more about the NPQR on our website at **www.ascp.org/npqr.**
For more information, contact Ali Brown, MD, FASCP, Chief Officer, Medical Quality, ASCP, at **NPQR@ascp.org**.


ASCP
NPQR
NATIONAL PATHOLOGY QUALITY REGISTRY

NPQR
NATIONAL PATHOLOGY QUALITY REGISTRY

CONTACT INFORMATION

Ali Brown, MD, FASCP
Chief Officer, Medical Quality, ASCP
NPQR@ascp.org

www.ascp.org/NPQR